UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/487,483	01/19/2000	Masue Shiba	04329.2217	3217

22852 7590 09/30/2003

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	4

DATE MAILED: 09/30/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/487,483	Applicant(s) SHIBA ET AL.	
	Examiner Michael J Simitoski	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 January 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15,17 and 18* is/are rejected.

7)☒ Claim(s) *16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 January 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-18 are pending.

2. No IDS was submitted.

Specification

3. The disclosure is objected to because of the following informalities:

   a. On page 32, lines 7 and 10, references to "RAS" should be "RSA".

   b. On page 35, line 16, "in stead" should be one word.

   c. On page 41, line 23, "x^{2i}" representing the dividend should be written as "x^{2k}" (replacing the 'i' with 'k').

   Appropriate correction is required.

Drawings

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference characters "22" (in the drawings) and "22a" (in the specifications) have both been used to designate "finite field GF(2^m) arithmetic controller".

A proposed drawing correction, corrected drawings or correction in the specifications on page 35, line 27, page 36, line 7 and page 37, line 2 are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

5. The drawings are objected to because in Fig. 14, "MODULAR" is misspelled "MODULER". A proposed drawing correction or corrected drawings are required in reply to the

Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim refers to a controller, but it is unclear from the specifications as to the specific function of the controller and the controller's function with regards to the apparatus claimed. Clarification is required.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an

international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

9. Claims 1-6, 9-11 and 17-18 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,230,179 to Dworkin et al. (Dworkin).

Regarding claims 1, 5 and 10, Dworkin discloses a "processor that combines finite field arithmetic and integer arithmetic", "providing operations required for [elliptic curve] cryptography" (see col. 1, lines 26-50). Dworkin further discloses that finite field addition is advantageous over integer arithmetic because no carries are produced (see col. 5, lines 32-47) and that it is necessary to implement carries in integer multiplication (see col. 7, lines 36-46). The carries in Dworkin's apparatus are held in register M during integer arithmetic operations (see col. 8, lines 15-23). The registers are chosen to hold enough to "handle at least the largest foreseeable F_2^m EC cryptosystem" and can be combined to support larger lengths (see col. 2, lines 63-67 and col. 3, lines 1-2).

Regarding claim 2, Dworkin discloses a processor, as described above, comprising finite field arithmetic circuitry and integer arithmetic circuitry whereby a mode control means selectively enables either the finite field circuitry or the integer arithmetic circuitry (see col. 1, lines 66-67 and col. 2, lines 1-3 and 42-56).

Regarding claims 3 and 9, Dworkin discloses an adder whose output is connected to an accumulator cell, which is used to store a partial product in the case of modular reduction. The adder adds the result of a previous step with the data in the accumulator (see fig. 6).

Regarding claim 4, Dworkin discloses, in Fig. 8, an adder circuit (element 170) that receives the carry from a previous iteration (time i-1), adds the carry to a current term and outputs a new carry back into register m_i at time i (element 182) (see col. 4, lines 58-67, col. 7, lines 36-67 and col. 8, lines 1-14).

Regarding claim 6, Dworkin discloses an integer arithmetic unit (see col. 1, lines 26-50), as described above, comprising a mode selection signal that selects whether the unit will implement finite field arithmetic or integer arithmetic (see col. 8, lines 11-23). Dworkin further discloses a carry input signal (see figure 8, element 180) that selects carry propagation (see col. 8, lines 10-14).

Regarding claim 11, Dworkin discloses a circuit as described above, "computing A*B mod M" wherein the circuit directs A to be multiplied by B and the result computed modulus M (see col. 10, lines 18-30).

Regarding claim 12, Dworkin discloses using a "brute force multiply" wherein a wide register of 2m bits is needed if the contents of two registers of size m are to be multiplied (see col. 10, lines 30-41).

Regarding claim 17, Dworkin discloses a "processor that combines finite field arithmetic and integer arithmetic", "providing operations required for [elliptic curve] cryptography" (see col. 1, lines 26-50) and specifically a processor that performs multiplication in a finite field (see col. 4, lines 58-67).

Regarding claim 18, Dworkin discloses an apparatus as described above, comprising a mode selection signal to select integer or finite field arithmetic (see col. 8, lines 10-14).

Dworkin further discloses that when performing integer arithmetic, carries are held in register M (see col. 8, lines 15-23).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dworkin et al. in view of U.S. Patent 3,064,896 to Carroll et al. (Carroll). Dworkin discloses an apparatus performing functions on polynomial coefficients in a finite field as described above, but lacks a method of iterative division as described in claim 13. Carroll teaches a method, and accompanying apparatus for division that allows adequate time for the maximum number of carries and eliminates unnecessary processing (see col. 2, lines 1-35). Carroll discloses an apparatus that divides through successive subtractions of the divisor from orders of the dividend until the division is complete and a remainder and all bits of the quotient are produced (see col. 1, lines 32-72 and col. 7, lines 35-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Dworkin's apparatus to include a division system that eliminates unnecessary processing, as taught by Carroll.

12. Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dworkin et al. in view of Carroll et al. (Carroll), in further view of U.S. Patent 5,468,297 to

Zook. Dworkin discloses an apparatus that performs modular multiplication, as modified above, but lacks multiplication of an inverse in place of a division operation. Zook teaches that division is a very complex operation in finite field arithmetic, as compared to multiplication, so it is beneficial to perform division by taking the multiplicative inverse of an element followed by a multiplication (see col. 1, lines 54-60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Dworkin's apparatus to perform division by first inverting an element then performing a multiplication to gain the benefit of avoiding a complex division operation, as taught by Zook.

Allowable Subject Matter

13. The following is a statement of reasons for the indication of allowable subject matter:

Claim 16 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The reason for allowance is such that the prior art relied upon fails to specifically point out a method of counting consecutive zeros, extracting one block and an additional 1 bit, obtaining an inverse of the two blocks and concatenating '0' bits and a single '1' bit to a first block and finally bit-shifting the result toward an upper order by the count of zeros recorded previously.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:30 p.m.. The examiner can also be reached on alternate Fridays from 8:00 a.m. – 4:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:
(703)746-7239 (for formal communications intended for entry)

Or:
(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

MJS
10 September 2003

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2134